IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	**MAIL STOP AF**
Christophe Clavier et al.	Group Art Unit: 2131
Application No.: 09/807,607	Examiner: Kaveh Abrishamkar
Filed: June 1, 2001	Confirmation No.: 2078
For: COUNTERMEASURE METHOD IN AN ELECTRONIC COMPONENT USING A SECRET KEY CRYPTOGRAPHIC ALGORITHM	

PRE-APPEAL BRIEF REQUEST FOR REVIEW

Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicants request review of the final rejection of claims 1-10 and 13-16 in the Office Action dated July 7, 2005. No amendments are being filed with this request.

This request is being filed with a Notice of Appeal.

The subject application contains two independent claims, 1 and 13. For the sake of brevity, this request will focus upon the issues presented by those two claims.

Claim 1

The claims are directed to countermeasures against external attacks that monitor cryptographic operations for the purpose of discovering secret information, such as keys that are used during the operations. An exemplary embodiment of the countermeasure is described with reference to the DES cryptographic algorithm. This algorithm comprises 16 computation rounds, which are respectively depicted in Figures 7-8 by the labels T1-T16.

Claim 1 recites a countermeasure method that includes the step of executing a first set of instructions in a cryptographic algorithm with a first manipulating means to deliver output data on the basis of input data. Referring to Figure 7, an example of this step is depicted in computation round T2, where the SBOX operation is executed with a first

manipulating means that is implemented with a constants table TC_0. An example of such a table is illustrated in Figure 6. The table receives a 6-bit input signal b1...b6, and produces a 4-bit output signal a1...a4.

Claim 1 recites the further step of executing another set of instructions "with other manipulating means that are derived from said first manipulating means by complementation of at least one of said input data and said output data." Referring again to Figure 7, during computation round T1, the SBOX operation is carried out with the constants table TC_1. An example of this table is illustrated in Figure 9. As can be seen, the output values a1...a4 in this table are the complements of the output values that are delivered by the table TC_0.

The rejection of claim 1 is based upon a combination of the Leppek and Kocher patents. As discussed in greater detail in Applicants' response filed May 12, 2005, the Leppek patent discloses a compound encryption scheme in which a plurality of different types of encryption routines are successively applied to data that is to be encrypted. In response to the Applicants' argument that the Leppek does not disclose that one of these encryption routines is derived from another one of the encryption routines, the final Office Action states that the sequence of encryption routines could comprise DES in the first instance, and triple DES in another instance. The Action states that triple DES is derived from DES, with reference to the Kocher patent at column 1, lines 46-55.

Applicants submit that the Leppek patent does not provide support for the purported interpretation. Nevertheless, even if one were to assume that the patent could be interpreted in such a manner, the result still does not lead to the claimed subject matter.

As pointed out in Applicants' previous response, claim 1 recites that the second, or "other ," manipulating means is derived from the first manipulating means "by complementation of at least one of said input data and said output data." The Office Action acknowledges that the Leppek patent does not disclose this claimed feature, and relies upon the Kocher patent at column 6, lines 29-63, and column 9, line 5-23, as disclosing the

"complementation of data" (Office Action at page 3, lines 2-6). However, neither of these portions of the patent describes, nor otherwise relates to, the "complementation" of data. Rather, as pointed out in Applicants' previous response, the Kocher patent discloses a technique wherein a message to be encrypted, and/or the encryption keys, are disguised, or "blinded," prior to processing by the DES algorithm.

The Office Action does not explain how this disclosure can be interpreted to suggest the "complementation" of input data or output data. As best as can be surmised, the Office Action appears to be referring to the exclusive-or (XOR) operation that are described in the referenced portions of the Kocher patent. However, an exclusive-or operation is not the same as complementation. Specifically, complementation employs a single input signal, e.g. a 1 or 0, and produces an output bit that is the complement of the input bit. In contrast, an exclusive-or operation requires *two* input signals, and produces an output signal that is dependent upon the *relationship* of the two input signals. The results of these two different operations are not the same.

Consequently, the final Office Action has not provided any support for the assertion that the Kocher patent discloses a manipulating means that is derived from another manipulating means by the complementation of input data and/or output data. As set forth in M.P.E.P. §2143.03, to establish a prima facie case of obviousness, "all the claim limitations must be taught or suggested by the prior art." Since the final Office Action does not identify any teaching of "complementation of data" in either of the Leppek or Kocher patents, it fails to establish a prima facie case of obviousness, for at least this reason.

Claim 13

Claim 13 recites an electronic component that provides countermeasures against attacks. This component has, among other elements, a processor that executes instructions in a cryptographic algorithm, in accordance with a selected one of a plurality of different

manipulating means stored in a program memory. The claim further recites "means for generating a random value for selecting the manipulating means to be employed during a given execution of said algorithm...." As pointed out in Applicants' previous response, the Leppek patent does not contain any teaching that the particular manipulating means, i.e. encryption routine, that is selected for a given execution of its algorithm is based upon a random value (see the paragraph bridging pages 10 and 11 of the response).

In responding to this argument, the final Office Action states:

> Leppek discloses a generation of an *random* access code sequence to call up one of the different data encryption operators to produce a sequence of data encryption operators (column 2, lines 24-38). This sequence is a random value, and it selects which manipulating means are to be used. (page 3, lines 14-18; emphasis added)

The referenced portion of the Leppek patent does not disclose how the access code sequence is generated. Specifically, it does not disclose that the access code sequence is *random.* In fact, the word "random" does not appear at all in the disclosure of the Leppek patent.

The only disclosure in the Leppek patent of a process for generating the access code sequence appears at column 4, lines 33-51. In this example, the number of encryption routines is equal to two. As can be seen, the generation of the access codes sequence results in an alternating sequence. This sequence is not random. Rather, it is a *predetermined* sequence.

The patent does not describe any other procedure for generating an access code sequence. In particular, it does not disclose that the generation of a sequence is carried out by generating a random value to select the various encryption routines.

As in the case of claim 1, the rejection of claim 13 is based upon an assertion that the references disclose a feature which, in fact, is not disclosed. Since all the claim limitations are not taught or suggested by the prior art, the final rejection fails to set forth a prima facie case of obviousness.

For at least the foregoing reasons, the final Office Action does not set forth a complete record that would form a proper basis for going forward with an appeal. In particular, it fails to show that all the limitations of the independent claims are taught or suggested by the prior art references. Accordingly, Applicants respectfully request that the final Office Action be withdrawn, and that all claims be allowed, or prosecution be reopened to establish a proper record for appeal.

Respectfully submitted,

BUCHANAN INGERSOLL PC

Date: November 7, 2005

By: _____
James A. LaBarre
Registration No. 28,632

P.O. Box 1404
Alexandria, Virginia 22313-1404
(703) 836-6620